What is claimed is:

1. 1. A method for conducting authenticated business transactions involving
2. microprocessor equipped devices over a distributed network, the method
3. comprising the acts of:
4.   a)   providing an on-line authentication service available on the distributed
5.   network;
6.   b)   authenticating a plurality of users to said on-line authentication service
7.   using a closed authentication system to produce a plurality of authenticated
8.   users; and
9.   c)   connecting a group of at least two of said plurality of authenticated users
10.   under persistent mediation of said on-line authentication service, producing
11.   a connected group.

1. 2. The method of claim 1 further comprising enrolling said users to said on-line
2. authentication service prior to authenticating said users to said on-line
3. authentication service.

1. 3. The method of claim 2 wherein persistent mediation of said connected group
2. comprises compiling an audit trail of an interaction of said connected group.

1. 4. The method of claim 3 wherein said closed authentication system is a pseudo-PKI
2. system of the type which cryptographically camouflages a user's private key in a
3. software container.

1. 5. The method of claim 4 wherein the on-line service is a persistent authentication
2. and mediation service.

95

1   6.   A method for conducting authenticated business transactions involving

2   microprocessor equipped devices over a distributed network, the method

3   comprising the acts of:

4   a)   providing an on-line authentication service available on the distributed

5   network;

6   b)   authenticating a plurality of users to said on-line authentication service

7   using a closed PKI authentication system to produce a plurality of

8   authenticated users; and

9   c)   connecting a group of at least two of said plurality of authenticated users

10   under persistent mediation of said on-line authentication service, producing

11   a connected group.

1   7.   The method of claim 6 further comprising enrolling said users to said on-line

2   authentication service prior to authenticating said users to said on-line

3   authentication service.

1   8.   The method of claim 7 wherein persistent mediation of said connected group

2   comprises compiling an audit trail of an interaction of said connected group.

1   9.   The method of claim 7 wherein said closed PKI authentication system is a pseudo-

2   PKI system of the type which cryptographically camouflages a user's private key in

3   a software container.

1   10.   The method of claim 9 wherein the on-line service is a persistent authentication

2   and mediation service.

1   11.   A method for conducting authenticated business transactions involving

2   microprocessor equipped devices over a distributed network, the method

3   comprising the acts of:

4   a)   providing a persistent authentication and mediation service as an on-line

5   service on the distributed network;

6   b)   enrolling users seeking enrollment in the persistent authentication and

7   mediation service, to produce a plurality of enrolled users;

8   c)   receiving requests from enrolled users for authentication to the persistent

9   authentication and mediation service;

10   d)   authenticating enrolled users seeking authentication to the persistent

11   authentication and mediation service using a closed PKI authentication

12   system, so as to maintain a plurality of authenticated users;

13   e)   receiving requests from authenticated users to be connected to particular

14   other authenticated users;

15   f)   connecting groups of at least two authenticated users under persistent

16   mediation of the persistent authentication and mediation service so that the

17   at least two authenticated users can conduct an interaction;

18   g)   repeating act (f) to produce a plurality of groups of connected users; and

19   h)   mediating the interaction among the at least two users of each of said

20   plurality of groups of connected users after connection, wherein the act of

21   mediating the interaction comprises the acts of providing authenticated

22   identity information to the interaction, directly compiling an audit trail of

23   the interaction and making information from the audit trail available to the

24   at least two users of each group of connected users.

1   12.   The method of claim 11 wherein the act of enrolling users seeking enrollment in

2   the persistent authentication and mediation service comprises the acts of:

3   a)   distributing software to a user seeking enrollment which enables

4   microprocessor equipped devices operated by the user seeking enrollment

5   to interact with said persistent authentication and mediation service,

6		b)	generating a unique private key, and a unique public key for the user
7			seeking enrollment,
8		c)	obtaining permanent credentials particular to each of the user seeking
9			enrollment, said credentials comprising public permanent credentials and
10			secret permanent credentials,
11		d)	deciding whether to approve the applicant seeking enrollment;
12		e)	distributing the unique public key and the unique private key to the user
13			seeking enrollment if the user seeking enrollment is approved, and
14		f)	storing said permanent credentials in a customer database, said customer
15			database being accessible to said persistent authentication and mediation
16			service, whereby the user seeking enrollment becomes one of said
17			multiplicity of enrolled users, and
18		g)	repeating steps (a) through (f) for each applicant seeking enrollment.

1	13.		The method of claim 12 wherein the act of authenticating enrolled users seeking
2			authentication to the common authenticating service comprises the acts of:
3		a)	generating a challenge message from the persistent authentication and
4			mediation service and sending it over the public network to an enrolled
5			user seeking authentication,
6		b)	receiving a response to the challenge from the user seeking authentication,
7			said response comprising an encrypted message and the unique public key
8			unique to the enrolled user seeking authentication,
9		c)	verifying the authenticity of the response to the challenge, the act of
10			verifying the authenticity comprising the act of decrypting the response
11			using the public key unique to the enrolled user seeking authentication to
12			produce a decrypted response,
13		d)	authenticating the enrolled user seeking authentication if the decrypted
14			response indicates that the response was authentic, whereby the enrolled
15			user seeking authentication becomes an authenticated user,

16   e)   rejecting the user if the decrypted response indicates that the response was

17   not authentic, and

18   f)   repeating steps (a) through (e) for each enrolled user seeking

19   authentication.

1   14.   The method of claim 13 further comprising the acts of:

2   a)   allowing authenticated users to optionally submit variable credentials;

3   b)   receiving variable credentials submitted by authenticated users;

4   c)   storing the variable credentials in the customer database according to user;

5   d)   providing authenticated users discovery software, whereby authenticated

6   users may dynamically discover enrolled users according to search criteria.

7   e)   granting authenticated users access to search the public permanent

8   credentials and the variable credentials in the customer database, using said

9   discovery software.

1   15.   The method of claim 14 further comprising making available collaboration

2   software to each of said plurality of groups of connected users is to facilitate

3   communication among the at least two authenticated users of each group, wherein

4   said collaboration software makes information from the audit trail available to each

5   of said at least two authenticated users of each of said plurality of groups of

6   connected users.

1

2   16.   The method of claim 15 wherein:

3   a)   the software PKI authentication system is a pseudo-PKI system of the type

4   which cryptographically camouflages the unique private keys in a software

5   container,

6   b)   wherein the unique public keys is encrypted in a form recognizable to the

7   common authentication agent and stored in a digital certificate,

8   c)   wherein the act of authenticating an enrolled user to the common

9   authenticating service further comprises the act of decrypting the encrypted

| 10 | | unique public key unique to the enrolled user prior to decrypting the |
| 11 | | response. |

1 17. The method of claim 16 wherein the persistent authentication and mediation
2 service is provided by at least one host site connected to the distributed network,
3 said at least one host site comprising at least one computer server operated by an
4 open software platform providing intelligent interactions, wherein the operation
5 the persistent authentication and mediation service is implemented by software
6 operating on the open software platform.

1 18. The method of claim 17 wherein interactions between users and the persistent
2 authentication and mediation service are mediated through the open software
3 platform.

1 19. The method of claim 18 wherein some of the plurality of groups of connected
2 users comprise at least three authenticated users.

1 20. The method of claim 19 wherein some of the plurality of groups of at least three
2 connected users comprise users of different types.

1 21. The method of claim 18 wherein the distributed network is the public Internet.
1
2 22. An online service for conducting business transactions among microprocessor
3 equipped devices over a distributed network, the online service comprising:
4 a) a host site connected to the network, the host site comprising an open
5 software platform providing intelligent interactions;
6 b) a persistent authentication and mediation service, the persistent
7 authentication and mediation service comprising a software PKI
8 authentication agent operating on said open software platform such that

9 communications over the network by said persistent authentication and

10 mediation service are mediated by said open software platform;

11 c) a customer database comprising permanent credentials and dynamically

12 variable information corresponding to users of the online service and a

13 database manager for managing the customer database;

14 d) software operating on said open software platform which performs at least

15 the following functions:

16 i) enrolling users seeking enrollment in the persistent authentication

17 and mediation service to produce enrolled users,

18 ii) storing credentials corresponding to enrolled users in the customer

19 data base,

20 iii) authenticating enrolled users seeking authentication to the

21 persistent authentication and mediation service to produce

22 authenticated users,

23 iv) allowing a authenticated users to discover enrolled users according

24 to search criteria,

25 v) allowing authenticated users to be connected under mediation of

26 the persistent authentication and mediation service through the

27 open software platform,

28 vi) allowing collaboration between authenticated users which have

29 been connected, and

30 vii) memorializing transactions between authenticated users.

1 23. The online service defined in claim 22 where the function of enrolling users

2 seeking enrollment in the persistent authentication and mediation service comprises

3 the functions of:

4 a) distributing software to a user seeking enrollment which enables

5 microprocessor equipped devices operated by the user seeking enrollment

6 to interact with the persistent authentication and mediation service,

7		b)	generating a unique private key, and a unique public key for the user
8			seeking enrollment,
9		c)	obtaining permanent credentials particular to each of the user seeking
10			enrollment, said credentials comprising public permanent credentials and
11			secret permanent credentials,
12		d)	deciding whether to approve the applicant seeking enrollment;
13		e)	distributing the unique public key and the unique private key to the user
14			seeking enrollment if the user seeking enrollment is approved, and
15		f)	storing said permanent credentials in a customer database, said customer
16			database being accessible to said persistent authentication and mediation
17			service, whereby the user seeking enrollment becomes one of said
18			multiplicity of enrolled users, and
19		g)	repeating steps (a) through (f) for each applicant seeking enrollment.

1	24.		The online service defined in claim 23 wherein the function of authenticating
2			enrolled users seeking authentication to the persistent authentication and mediation
3			service comprises the functions of:
4		a)	generating a challenge message from the persistent authentication and
5			mediation service and sending it over the public network to an enrolled
6			user seeking authentication,
7		b)	receiving a response to the challenge from the user seeking authentication,
8			said response comprising an encrypted message and the unique public key
9			unique to the enrolled user seeking authentication,
10		c)	verifying the authenticity of the response to the challenge, the act of
11			verifying the authenticity comprising the act of decrypting the response
12			using the public key unique to the enrolled user seeking authentication to
13			produce a decrypted response,
14		d)	authenticating the enrolled user seeking authentication if the decrypted
15			response indicates that the response was authentic, whereby the enrolled
16			user seeking authentication becomes an authenticated user,

102

17	e)	rejecting the user if the decrypted response indicates that the response was
18		not authentic, and
19	f)	repeating steps (a) through (e) for each enrolled user seeking
20		authentication.

1 25. The online service defined in claim 24 wherein:

2 a) the software PKI authentication agent is a pseudo-PKI system of the type

3 which cryptographically camouflages each of the unique private keys in a

4 software container,

5 b) wherein each of the unique public keys is encrypted in a form recognizable

6 to the common authentication agent and stored in a digital certificate,

7 c) wherein the function of authenticating an enrolled user to the common

8 authenticating service further comprises the function of decrypting the

9 encrypted unique public key unique to the enrolled user prior to decrypting

10 the response.

1 26. The online service defined in claim 25 wherein the distributed network is the public

2 Internet.

1 27. A system for conducting business transactions over a distributed network, the

2 system comprising:

3 a) a persistent authentication and mediation service site providing a persistent

4 authentication and mediation service, said site connected to the public

5 network, said site comprising

6 i) a open software platform application providing intelligent

7 interactions said platform application mediating all interactions of

8 said persistent authentication and mediation service site via said

9 public network,

10 ii) anauthentication agent application comprising a software pseudo-

11 PKI authentication application operating on said open software

103

12			platform application, said common authentication agent application
13			comprising software which enrolls new businesses users producing
14			enrolled users and authenticates the enrolled users,
15		iii)	an audit agent application operating on said open software platform
16			which logs and monitors interactions mediated by the open
17			software platform,
18		iv)	a discovery software application operating on said open software
19			platform, and
20		v)	a collaboration software application operating on said open
21			software;
22	b)		a multiplicity of user sites operated by the enrolled users, the user sites
23			being connected to the public network, each site operating at least one
24			computer application whereby it may interact with other business users and
25			each site further comprising software which allows interaction with the
26			persistent authentication and mediation service, a software camouflaged
27			private key, and a digital certificate, said digital certificate comprising an
28			encrypted pseudo-public key recognizable to said persistent authentication
29			and mediation service;
30	c)		a database of authentication information pertaining to the enrolled business
31			users of said persistent authentication and mediation service, the database
32			accessible to the common authentication application.

1   28.   The system defined in claim 27 further comprising a plurality of authentication

2   provider applications accessible by the authentication agent application.

1   29.   The system defined in claim 28 wherein at least one authentication provider

2   application is located at a different site than the persistent authentication and

3   mediation service site.

1   30.   The system defined in claim 28 further comprising a plurality of audit provider

2   applications accessible by the audit agent application.

1   31.   The system defined in claim 29 wherein at least one authentication application

2   provider is located at a different site than the persistent authentication and

3   mediation service site.

1   32.   The system defined in claim 29 wherein the network is the public Internet.

1   33.   The system defined in claim 31 wherein the network is the public Internet.

1   34.   The system defined in claim 33, wherein the user sites comprise sites which are

2   chosen from the group consisting of user sites which access the network via a

3   browser operating on a computer, mobile telephonic devices which access the

4   network, world wide web sites, and sites comprising applications without a user

5   interface.

1   35.   An apparatus for providing a service for conducting authenticated business

2   transactions involving a multiplicity of users over a distributed network, the

3   apparatus comprising:

4   a)   at least one application server connected to the public network, the at least

5   one application server having a computer processor and a computer

6   readable memory, the memory storing the software to implement the

7   service, the software comprising

8   i)   an open software platform providing intelligent interactions,

9   ii)   a software pseudo-PKI authentication agent application, operating

10   on said open software platform,

11   iii)   a discovery software application, operating on said open software

12   platform, and

13   iv)   a collaboration software application, operating on said open

14   software platform,;

15   b)   at least one database server, the at least one database server comprising a

16   business users database, the business users database comprising

17   i)   authenticated data about registered business users, said

18   authenticated data being protected from user modification;

19   ii)   data pertaining to registered business users which is dynamically

20   modifiable by said business users; and

21   iii)   data needed for linking business users;

22   whereby the application server facilitates authenticated interactions

23   between business users, including the ability to access other authenticated

24   users without repeated logging in, the ability to dynamically search for

25   authenticated users according to user defined specifications, and

26   accomplish peer to peer collaboration.

1   36. An apparatus as defined in claim 35 where the distributed network is the Internet.